Economist Intelligence Unit

TECNOLOGIA

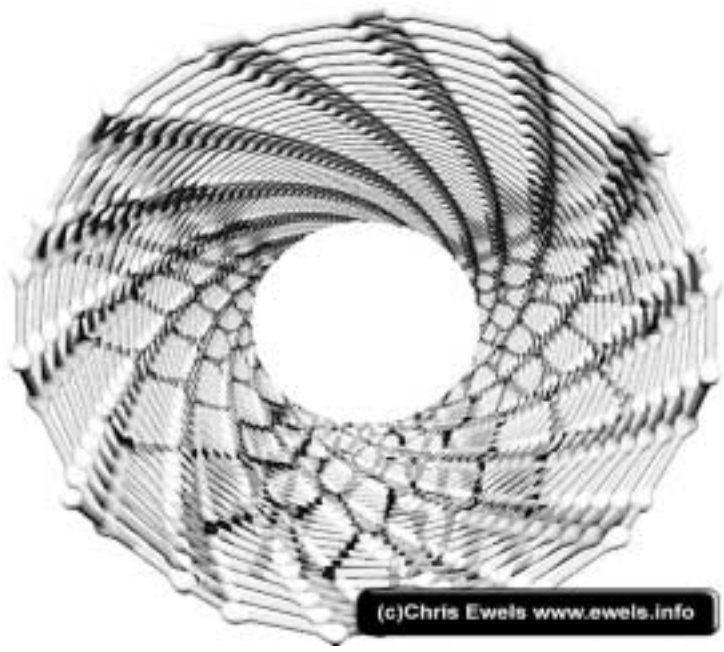
COMPUTADORAS CUANTICAS, LOS SISTEMAS DEL FUTURO

Esta tecnología tendría repercusión inmediata en el comercio, la banca y el espionaje

Manipulan con facilidad números astronómicos que inutilizarían una computadora ordinaria

CUAUHTÉMOC VALDIOSERA

Una rama emergente de la nueva computación la constituye el advenimiento de las computadoras cuánticas, lo cual parece que podrá ser una realidad en los próximos años. A mediados de los años noventa varias empresas comenzarán a llevar a cabo investigaciones cuánticas. Fujitsu Quantum Devices se creó en 1991. IBM formó un equipo de investigación cuántica en 1993, bajo la supervisión de Charles Bennett, uno de los precursores en la materia. ATT y otras compañías siguieron pronto sus pasos, al igual que otros centros universitarios, como el CalTech o instituciones estatales como los Alamos.



El tema fue planteado originalmente como una posibilidad por el célebre físico Richard Feynmann –el mismo genio que previó los desarrollos nanotecnológicos– en un artículo publicado en 1981. Feynmann se preguntaba hasta dónde podría reducirse el tamaño de las computadoras. Cuando éstas alcanzaran la dimensión de los átomos, razonaba, responderían a un conjunto totalmente nuevo de leyes completamente ajenas a la experiencia corriente. A Feynmann le frustraba que muchos de los problemas fundamentales de la teoría cuántica no pudieran resolverse mediante computadoras ordinarias. Muchos de los objetos que se encuentran en la física cuántica requieren un número infinito de cálculos, que está por tanto mas allá de la capacidad de las computadoras ordinarias.

La solución de Feynmann fue sencilla: ¿por qué no utilizar una computadora cuántica para resolver problemas cuánticos? Sus ideas cobraron finalmente forma concreta en un ensayo de David Deutch, de la Universidad de Oxford, en 1985. Deutch se dio cuenta de que los procesos cuánticos son como gigantescas máquinas sumadoras. La única diferencia es que las computadoras cuánticas manejan regularmente cantidades infinitas en un abrir y cerrar de ojos.

Las computadoras cuánticas son totalmente diferentes de las ordinarias, pues cálculos que requieren gran cantidad de tiempo pueden ser procesados rápidamente en ellas. Una computadora cuántica no es una máquina de Turing y es esencialmente distinta de una posible computadora de ADN o molecular, que pueden procesar una cantidad enorme de información, pero sólo finita, utilizando números inmensos de moléculas que actúan en paralelo.

En 1994 se produjo gran expectación cuando Peter Shor, de los laboratorios AT&T, logró un importante avance en la informática cuántica al demostrar que si se podía construir una computadora cuántica, ésta podría descomponer rápidamente en factores cualquier número sin importar su longitud. Así, una computadora cuántica tendría repercusión inmediata en el comercio, la banca y el espionaje. Algunas de sus transacciones secretas se basan en el difícil problema de reducir a factores un número que puede tener hasta 100 dígitos. Dado que las computadoras reducen a factores los números grandes, principalmente mediante un proceso de ensayo y error, normalmente tardaría décadas resolver estos problemas cuando los números rebasaran 200 dígitos. Sin embargo, una computadora cuántica, demostraba Shor, puede resolver fácilmente este problema.

Para situar esto en perspectiva, pensemos que fueron necesarios ocho meses para que mil 600 computadoras de todo el mundo, conectadas a través de Internet, descompusieran en factores un número de 129 dígitos.

Esa batería de computadoras tardaría siglos en descomponer en factores un número de 250 dígitos; si se pusiera por escrito, el razonamiento requeriría un 10 elevado a la potencia 500 de líneas en papel. Para hacerse una idea de la magnitud de esta monstruosa cantidad, pensemos nada más que el número total de átomos en el universo visible equivale a un 10 elevado a la potencia 80.

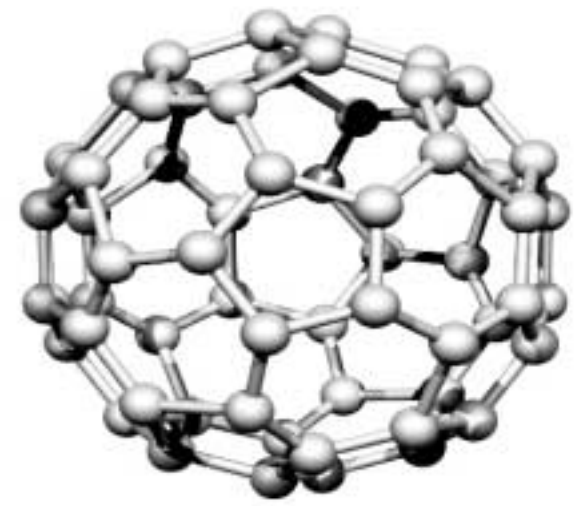
En principio, la teoría cuántica ha sumado todos los caminos posibles que el fotón podría atravesar y todos los estados de rotación posibles. Pero el número de estos estados posibles de una serie de mil átomos es 2 elevado a la milésima potencia, es decir, aproximadamente un uno seguido de 300 ceros. Una vez más, esta cifra es muy superior al número de átomos del universo visible. Así pues, una computadora cuántica puede manipular fácilmente números astronómicos que inutilizarían una computadora ordinaria.

Si las computadoras cuánticas son infinitamente más potentes que las supercomputadoras más grandes, y si pueden descifrar códigos de cifrado por valor de cientos de miles de millones de dólares, ¿por qué no se ha puesto en marcha un programa intensivo para construirlas?

Una de las causas principales ha sido el problema de que la menor impureza o contaminación procedente del mundo exterior podría alterarla. La computadora cuántica deberá estar aislada de toda posible interacción con el mundo exterior, tarea sumamente difícil. En principio, incluso un solo rayo cósmico que atravesara la computadora cuántica podría interferir en el número infinito de cálculos que realiza. Las sondas espaciales requieren “salas limpias“ para que ni siquiera las partículas de polvo alteren los delicados giroscopios. Las computadoras cuánticas, en comparación, deberán estar aisladas incluso de las partículas subatómicas perdidas.

El progreso en esta dirección es lento, pero se está acelerando. David Deutch comentó en una entrevista concedida a *Discover* en su página web, hace ya cinco años: “el avance tecnológico en esta área me ha dejado atónito en los últimos años. Cuando la gente me hacía esta pregunta hace tres o cuatro, solía decir que era cuestión de siglos. Ahora soy mucho más optimista”.

En esa misma ocasión, Seth Lloyd, del MIT, había señalado: “es tan difícil como unir una serie de átomos. Se trata de objetos extremadamente pequeños y sensibles. Pero el ser humano está llegando al punto en que pueda controlar estas cosas. Es un gran juego de dados tecnológico. En un futuro no tan lejano, quizá será posible realizar cálculos plenamente cuánticos”. Cosa que se ha confirmado con el anuncio de la IBM.



El optimismo de ambos científicos se basaba en avances claves en dos laboratorios, que están fabricando algunos de los componentes de una computadora cuántica. El trabajo corre a cargo de Jeff Kimble en el Tecnológico de California, el Caltech, y David Wineland y Chris Monroe en el Instituto Nacional de Normas y Tecnologías de Boulder, Colorado.

En el experimento de la segunda institución se comienza con una serie de átomos de mercurio dispuestos en fila. Cada átomo de mercurio gira hacia arriba o hacia abajo. Cuando se dirige un haz láser a la fila, puede introducir un átomo de mercurio que rote hacia abajo en uno que rote hacia arriba. En principio el haz láser que ha golpeado contra la línea de átomos de mercurio tiene en su interior la información sobre todos los estados posibles de la serie.

Internet cuántica, el futuro

El problema que la mayoría de los científicos enfrenta al tratar de desarrollar una computadora cuántica es ordenar los átomos en estos extraños estados mecánicos, para que puedan servir como *qbitios*. Fabricar aparatos con unos cuantos átomos, como el caso de la computadora cuántica desarrollada por IBM, no es ya tan difícil; pero construirlos con los 50 o más átomos que se necesitan para resolver problemas complejos parece tarea casi imposible. Pero ¿qué ocurriría si en vez de una computadora con 50 *qbitios* fuera posible conectar cinco procesadores que contuvieran 10 de estas unidades cuánticas? Es allí donde intervienen personas como Jeff Kimble y su proyecto de red cuántica, lo que permite prever que un futuro no muy lejano estaremos hablando de una Internet cuántica muy poderosa.

Como dice el mismo Kimble: “aunque apenas estamos comenzando con esto de la computación cuántica, nadie puede saber a qué mundo maravilloso nos conducirá este nuevo camino en que ya nos encontramos”.

Una computadora cuántica puede realizar operaciones infinitamente más complejas que las computadoras actuales. Así, en teoría, una computadora cuántica podrá resolver en 30 segundos problemas para los que el más veloz de los procesadores actuales demoraría miles de años.

Traducción de textos: Jorge Anaya